DECLARATION OF SENIOR SPECIAL AGENT TIMOTHY WILLIAMS

I, Timothy Williams, Senior Special Agent (SSA) of the United States Secret Service (USSS), assigned to the Raleigh Resident Office of the USSS, pursuant to 28 U.S.C. § 1746 and the laws of the United States, hereby declares under penalty of perjury that the following is true and correct to the best of my knowledge and belief:

INTRODUCTION

1. This declaration is made in support of a complaint to forfeit funds previously seized from a virtual currency (VC) account. This account contains proceeds and/or comingled funds of a cryptocurrency investment fraud scheme, whereby one or more criminal fraudsters used a fraudulent cryptocurrency exchange to commit wire fraud by inducing a victim known as E.B. to send money to a VC address controlled by the fraudsters. Once they received the VC, it was rapidly transferred to numerous other VC wallets, some of which ended up at accounts at the cryptocurrency exchange Binance. The USSS previously obtained a seizure warrant pursuant to 18 U.S.C. § 981(b) to bring traceable proceeds and other comingled funds involved in money laundering into government custody and now submit this declaration to support the funds' forfeiture.

DECLARANT'S BACKGROUND AND EXPERIENCE

2. I am a Senior Special Agent (SSA) with the United States Secret Service (USSS) assigned to the Raleigh (NC) Resident Office. I have been employed with the USSS as a Special Agent since June 2007. I have completed extensive training at both the Criminal Investigator Training Program at the Federal Law Enforcement Training Center, Glynco, GA and the Special Agent Training Course at the USSS training facility located in Beltsville, MD. This training included instruction in general law enforcement and criminal investigations to include violations

GOVERNMENT EXHIBIT A

of Title 18, United States Code, section 1343 (Wire Fraud). During my time with the Secret Service, I have conducted numerous financial crime investigations involving cryptocurrency and other financial instruments.

3. In my official capacity as a Special Agent, I have obtained the information set forth in this declaration through personal knowledge and/or directly from persons having knowledge of the facts of this case, including, as relevant, from speaking with, or review of sources of information or other law enforcement personnel.

PURPOSE OF THE DECLARATION

4. I make this declaration in support of the civil forfeiture of the proceeds of a criminal scheme to defraud E.B. executed in violation of 18 U.S.C. § 1343 and co-mingled funds that were involved in the unlawful laundering of such property in violation of 18 U.S.C. § 1956 and 1957. Specifically, this declaration supports the civil forfeiture of the following assets that were previously seized and brought into government custody on June 20, 2023:

a. 39,991.998502 USDT virtual currency (formerly held in Binance Holdings Ltd. Account with User ID #28892515, belonging to Pan Xuexia, and associated with deposit address 0x69bAfA83E44057A5d6a2684aff4Bc361Fc09a5ef) [hereafter "SUBJECT ACCOUNT"])

5. As explained below, the foregoing funds represent directly traceable criminal proceeds and/or money involved in the laundering of those proceeds, which were derived from a criminal fraud scheme that successfully defrauded E.B. by impersonating a legitimate cryptocurrency exchange and inducing E.B. to transfer VC belonging to him to accounts belonging to the fraudster(s).

FACTS SUPPORTING FORFEITURE

6. This investigation has determined that there is probable cause to believe that, beginning on or about December 27, 2022 within the Eastern District of North Carolina and elsewhere, a suspect identified by the name "Kelly" committed wire fraud on E.B., a resident of Fayetteville, North Carolina. Kelly defrauded E.B. of approximately 398 ETH (Ether virtual currency), which were collectively worth approximately $636,004 at the time of the transactions. As set forth more fully herein, Kelly convinced E.B. that E.B. was engaged in an online relationship with Kelly and that Kelly was a successful investor. Kelly also convinced E.B. to use the cryptocurrency exchange, "Crypto.com" to buy ETH and subsequently send the ETH to a purported cryptocurrency exchange located at the URL "https://www.daytradingwalletss.xyz." The investigation showed that this website was impersonating the legitimate cryptocurrency exchange Kraken. Thereafter, at the direction of Kelly, E.B. purchased ETH via the Crypto.com cryptocurrency exchange and sent it to the fraudulent Kraken platform in a series of transactions from December 27, 2022 to January 27, 2023. In addition E.B. was told by a purported customer service representative at the fraudulent Kraken exchange that he was required to pay "taxes" and an "insurance fee" in order to conduct a withdrawal of his funds. This led to E.B. sending additional ETH to the fraudulent Kraken exchange. As part of the investigation, USSS agents and analysts traced the ETH transactions made by E.B. This led to the subsequent seizure of two Binance accounts containing approximately $136,310 worth of cryptocurrency, one of which is the SUBJECT ACCOUNT referenced in this Declaration.

BACKGROUND OF CRYPTOCURRENCY

7. Based on my training, research, education, and experience, I am familiar with the following relevant terms and definitions:

8. **Cryptocurrency and Blockchain Generally**: Cryptocurrency, a type of virtual currency, is a decentralized, peer-to peer, network-based medium of value or exchange that may be used as a substitute for fiat currency to buy goods or services or exchanged for fiat currency or other cryptocurrencies.[1] Examples of cryptocurrency are Bitcoin, Litecoin, and Ether. Each unit of cryptocurrency is often referred to as a "coin" or "token." Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or in cloud-based servers. Users of cryptocurrency use public and private keys to transfer cryptocurrency from one person or place to another. A public key is typically a set of numbers and/or letters that a cryptocurrency user shares with other users to engage in a transaction in cryptocurrency, whereas a private key is typically a set of numbers and/or letters that the user of an account maintains privately to access his or her cryptocurrency. Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange, or through other intermediaries. Generally, cryptocurrency is not issued by any government, bank, or company; it is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. As such, most cryptocurrencies have a "blockchain," which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction.[2] Although many cryptocurrencies are or purport to be pseudonymous, often law enforcement and currency exchangers can use the blockchain to analyze transactions in cryptocurrency, identify individuals who are using cryptocurrency platforms for illicit purposes, and trace fraud proceeds from victims to one or more exchanges or wallets, discussed more fully below.

---

[1] Fiat currency is currency issued and regulated by a government such as the U.S. Dollar, Euro, or Japanese Yen.

[2] Some cryptocurrencies operate on blockchains that are not public and operate in such a way to obfuscate transactions, making it difficult to trace or attribute transactions.

9. **Wallets:** Cryptocurrency is often stored in a virtual account called a wallet, which can exist in, among other forms, an external computer device, a computer, on an application, or online. Wallets are software programs that interface with blockchains and generate and/or store public and private keys used to send and receive cryptocurrency. Access to a wallet and the cryptocurrency therein is typically protected by a password only known to the owner or user of the wallet. Wallets can be either "custodial" or "non-custodial" (also referred to as "centralized" or "decentralized"). In the case of a non-custodial wallet, the owner of the wallet has sole control of the wallet's private keys, which enable access to the wallet and any funds contained therein. With a custodial wallet, another party controls the private keys to the wallet. This is usually a cryptocurrency exchange (see below), and the relationship between the exchange and the customer can be considered analogous to the relationship between a traditional bank and its customers, where the bank securely maintains funds deposited by a bank customer.

10. **Exchanges/Exchangers:** Virtual currency "exchangers" and "exchanges", such as Binance, Coinbase, and Kraken, are individuals or companies that exchange virtual currency for other currencies, including U.S. dollars. Exchanges facilitate the purchase, sale, and transfer of a variety of digital currencies. Exchanges can identify accounts using a variety of target identifiers.

11. **Centralized/Decentralized Exchanges:** Centralized exchanges generally maintain a custodial role for the wallets of its customers, and function as trusted intermediaries in cryptocurrency transactions. Decentralized exchanges are commonly used to trade cryptocurrencies in a non-custodial manner, without the need for an intermediary to facilitate the transfer and custody of funds. Decentralized exchanges are often used to trade, or "swap", one type of cryptocurrency for another, for which the user pays a transaction fee.

12. **Chain-hopping:** Chain-hopping is a technique used to conceal the original source of cryptocurrency and to make it more difficult for law enforcement to trace the movement of cryptocurrency. It consists of converting one form of cryptocurrency for another, often multiple times in rapid succession. Chain-hopping is a primary technique in the laundering of stolen cryptocurrency or cryptocurrency obtained from illegal activity. Decentralized exchanges are often used in chain-hopping, as they allow one type of cryptocurrency to be converted to another while requiring the user to provide minimal or no identifying information.

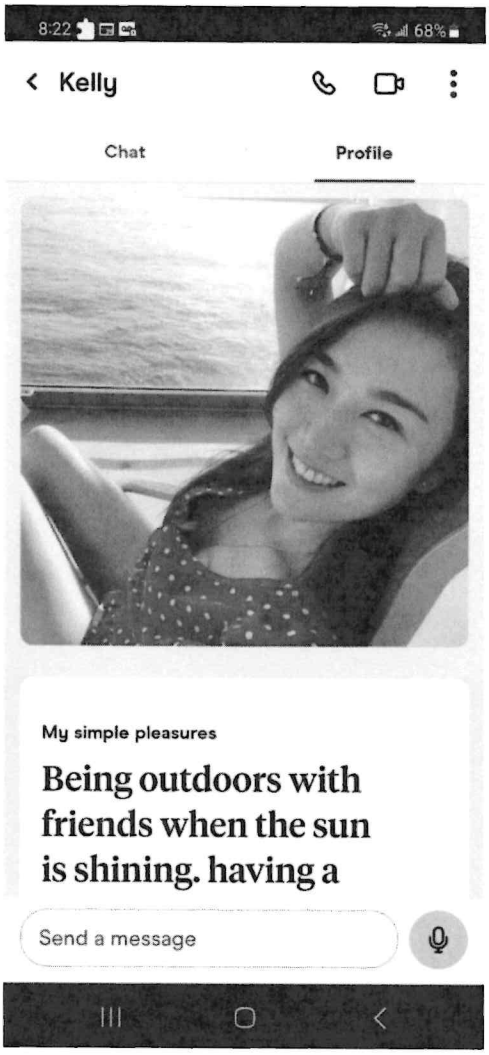
13. **Stablecoin:** Stablecoins are a type of cryptocurrency that has a price coordinated to a specific reference asset. The reference asset may be fiat money, another cryptocurrency, commodities, or other assets. Two common examples of stablecoins are Tether (USDT) and USD Coin (USDC). Both of these stablecoins are pegged to the U.S. dollar and are designed to maintain the value of $1 USD per coin.

FRAUD SCHEME INVOLVING VICTIM E.B.

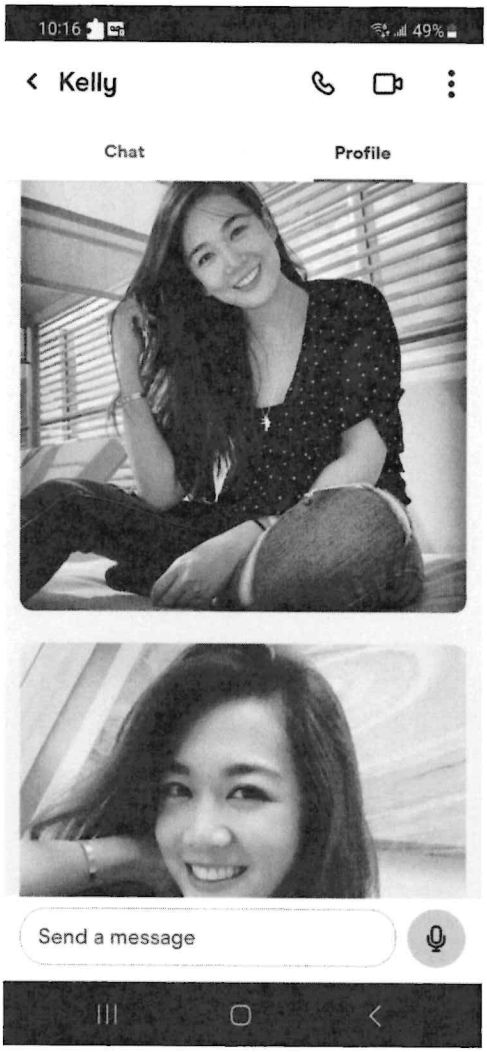
14. The information set forth below is derived from interviews with E.B. and investigation of publicly available cryptocurrency blockchain information.

15. On or about December 27, 2022, within the Eastern District of North Carolina and elsewhere, a suspect identified by the name "Kelly" committed wire fraud on a victim identified herein as "E.B." E.B. is a 28 year-old resident of Fayetteville, North Carolina. In or around December 2022, without prompting from E.B., a person claiming to be a woman named Kelly contacted E.B. on the dating application Hinge. They began a conversation, and Kelly asked them to move the conversation to the encrypted chat app Telegram. Kelly then began talking to E.B. about her cryptocurrency investments. Kelly advised E.B. how he could make a large profit by using a cryptocurrency exchange called "Kraken", and gave him instructions on how to start

investing. Of note, there is a legitimate cryptocurrency exchange called "Kraken", which uses the URL "kraken.com". Based on the investigation and my experience with similar fraud schemes, I believe that the suspects in this case used the name Kraken in order to appear legitimate, while actually being a fraudulent exchange that only existed to further this investment fraud scheme.



1- Hinge profile used by "Kelly"

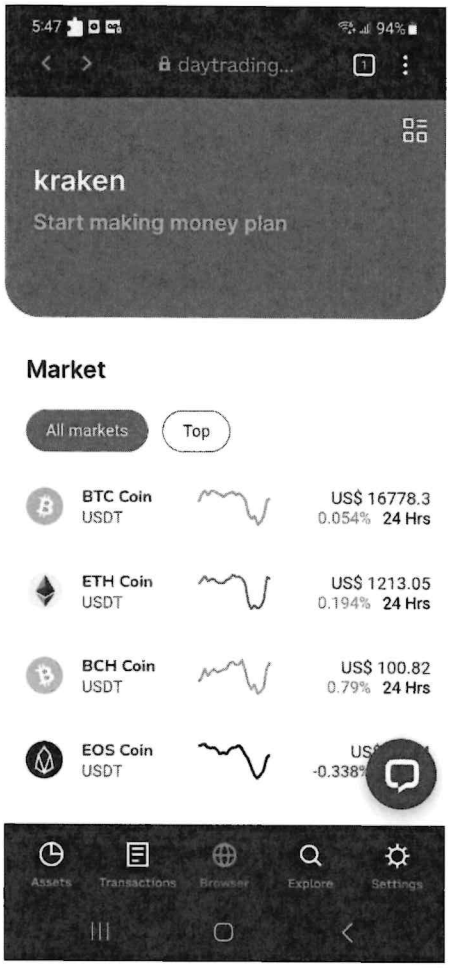


2- Hinge profile used by "Kelly"

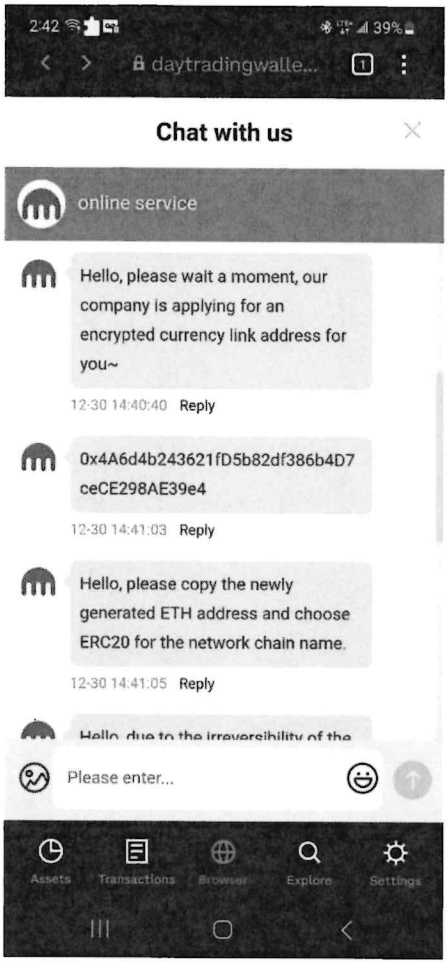
16. Kelly instructed E.B. to download the Crypto.com and Coinbase Wallet apps on his phone. Crypto.com is a legitimate cryptocurrency exchange, and Coinbase Wallet is an app that allows users to set up a self-hosted wallet that is not connected to the Coinbase exchange. The Coinbase Wallet app also has a browser that lets users utilize decentralized applications, or "dapps." Dapps are similar to a typical app found on a smartphone, but use blockchain technology to manage user data and maintain it in a decentralized way. On the Coinbase Wallet browser,

dapps can be accessed by clicking on icons, or by typing in a specific dapp address, similar to typing in a URL in a web browser.

17. Kelly then instructed E.B. to open an account on the legitimate cryptocurrency exchange Crypto.com and connect it to his personal bank account, which he did. She then told him to use Coinbase Wallet's Dapp browser to access the URL "https://www.daytradingwalletss.xyz", which he was told was a way to use the Kraken crypto exchange. In this dapp, which was built to resemble a typical crypto exchange website or app, the Kraken name and logo were displayed, indicating to the user that they were using a legitimate exchange. The dapp also had functionality similar to an exchange app, and E.B. was able to establish an account and request an address which he could use to deposit cryptocurrency into his account.



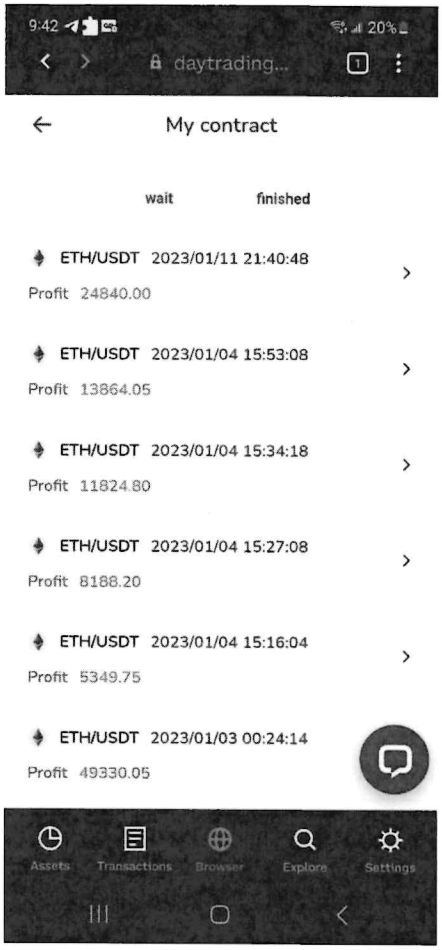
3- Fraudulent Kraken exchange Dapp – main page



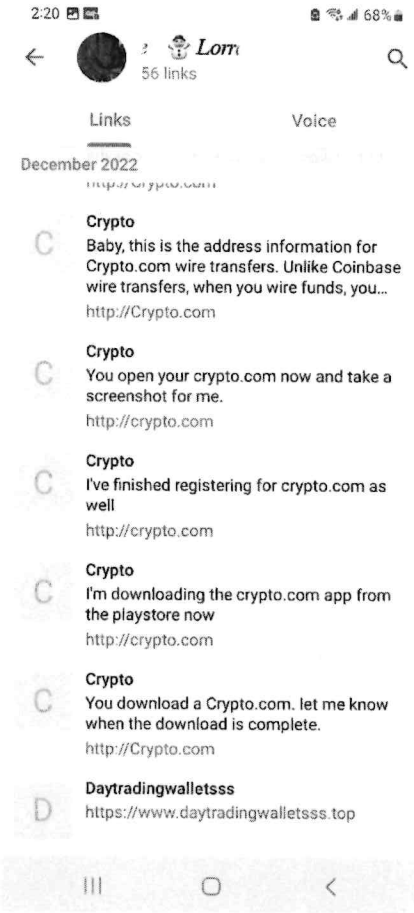
4- Fraudulent Kraken exchange Dapp - customer service chat providing an ETH deposit address

18. Kelly further instructed E.B. to purchase Ether (ETH) cryptocurrency on Crypto.com. and send the ETH to the address provided by the fraudulent Kraken dapp, which E.B. did using the Crypto.com app. Kelly provided E.B. with instructions on when to invest, which he was told would provide him a high rate of return on his investment. E.B. followed her instructions and was able to see what he believed were large profits by using the fraudulent Kraken dapp in the Coinbase Wallet app. She informed E.B. that he would be able to withdraw funds from Kraken and transfer them back to Crypto.com, where he would be able to sell the ETH for U.S. dollars. E.B. followed

this process and conducted his first transaction, using the process outlined above, to transfer 20.2271 ETH to the fraudulent Kraken exchange on December 27, 2022.



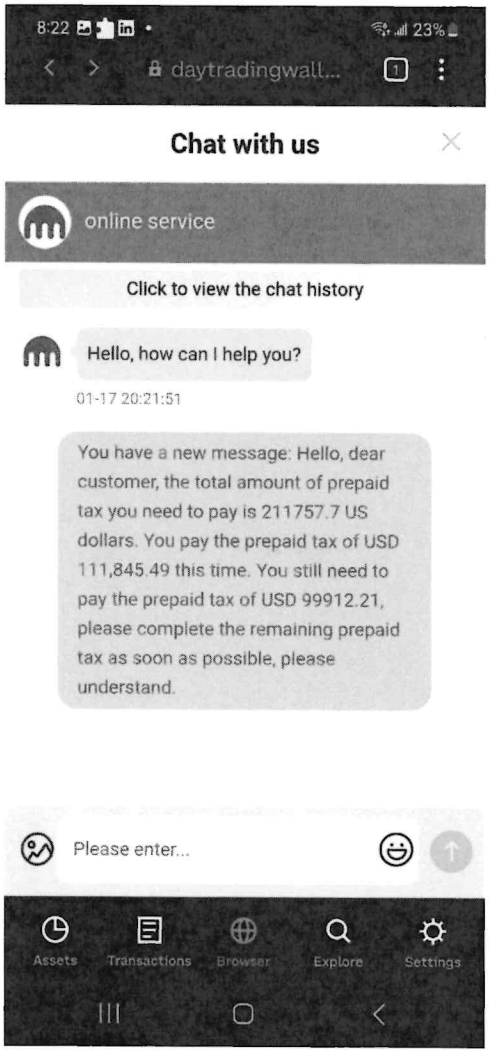
5- Fraudulent Kraken exchange Dapp - E.B.'s transactions and purported profits



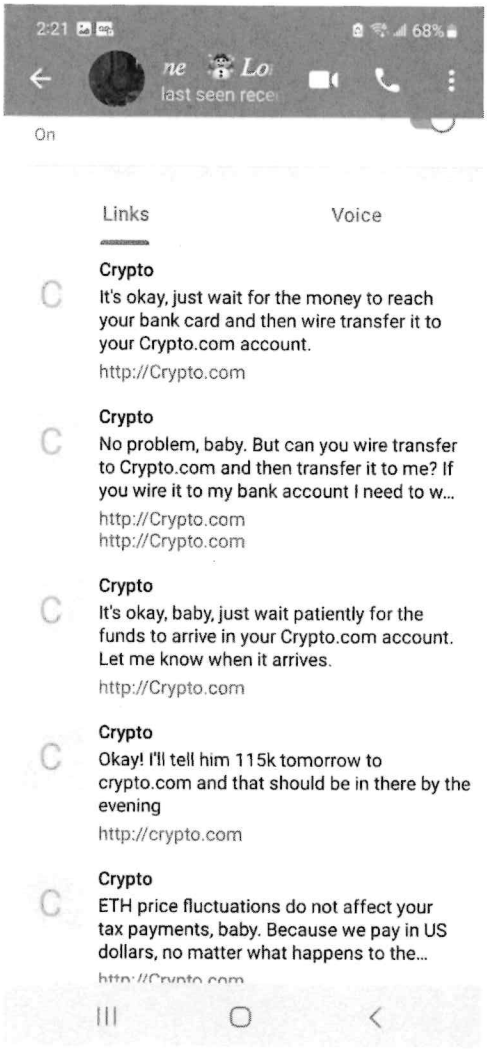
6- "Kelly" providing instructions to E.B. on the "investment" process

19. At Kelly's urging, E.B. continued to invest larger amounts, using the same process to transfer a total of approximately 398 ETH from December 27, 2022 to January 27, 2023 (valued at approximately $636,004 as of January 27, 2023). This total includes E.B.'s initial "investments", as well as "taxes" and an "insurance fee", which the fraudulent Kraken exchange's customer service informed him he was required to pay in order to withdraw any of his funds. E.B. was informed that he could not pay these taxes and fees from the account balance, and had to pay them separately by sending ETH to the same cryptocurrency address as his initial investment. Kelly also continued to encourage E.B. to pay the taxes and fees, and told him that she had been

able to withdraw funds with no issues. This caused E.B. to send additional funds to the scammers, as he was unaware that Kelly and the scammers were part of the same group. After paying the required taxes and fees, E.B. was still not able to withdraw any funds from his account. At that point he was asked for further fees in order to conduct a withdrawal, which he did not pay. All payments made by E.B. were sent to ETH addresses provided by the fraudulent exchange, all belonging to decentralized wallets which E.B. believed were deposit addresses for his Kraken account based on information he was provided on the fraudulent Kraken dapp.



7- Fraudulent Kraken exchange Dapp – customer service chat informing E.B. of required "tax" payments in order to conduct a withdrawal



8- "Kelly" encouraging E.B. to pay the "tax"

20. One of E.B.'s ETH transfers was traced to the SUBJECT ACCOUNT at Binance, as detailed below:

21. On January 20, 2023, E.B. transferred approximately 49.463 ETH from his Crypto.com wallet to the address provided by the fraudulent Kraken exchange. From January 20, 2023 to March 22, 2023, the funds were moved between several decentralized wallets, as detailed below, while being comingled with additional cryptocurrency and converted to different forms. On March 22, 2023, 200,000 USDT was sent to Binance wallet address

0x69bAfA83E44057A5d6a2684aff4Bc361Fc09a5ef. This is a deposit address for the SUBJECT ACCOUNT. As of March 22, 2023, when law enforcement requested Binance to freeze the account, approximately 39,996 USDT was present in SUBJECT ACCOUNT, which can be traced as proceeds directly from the victim.

22. Summary of the transfers from E.B. to SUBJECT ACCOUNT (for clarity, all subsequent cryptocurrency addresses have been shortened to the first eight characters):

a. 1/20/2023: 49.463258555 ETH was sent from E.B.'s Crypto.com account to 0x30bFE5 (address provided to victim by fraudulent Kraken exchange).

b. 1/20/2023: 49.463258555 ETH sent from 0x30bFE5 to 0xEBC1F4 (decentralized wallet). While in this wallet the ETH is comingled with additional funds.

c. 1/21/2023: 109 ETH sent from 0xEBC1F4 to 0xA53465 (decentralized wallet). While in this wallet the ETH is comingled with additional funds.

d. 1/21/2023: 162 ETH sent from 0xA53465 to 0x335c88 (decentralized wallet). While in this wallet the ETH is comingled with additional funds.

e. 1/21/2023: 169 ETH sent from 0x335c88 to 0x61F9Ef. 163 of this ETH are then sent to decentralized exchange Tokenlon and converted to USDT (minus a fee), then sent back to 0x61F9Ef as 268,712 USDT, where it is comingled with additional USDT and sent back to previous address 0x335c88 as 600,000 USDT.

f. 1/25/2023: 80,000 USDT sent from 0x335c88 to 0x835fD1 (decentralized wallet). While in this wallet the USDT is comingled with additional funds.

g. 1/25/2023: 800,000 USDT sent from 0x835fD1 to 0x5bB8dA (decentralized wallet).

h. 1/25/2023: 310,000 USDT sent from 0x5bB8dA to 0x1dC08a (decentralized wallet).

i. 1/26/2023: 199,965 USDT sent from 0x1dC08a to 0x070a83 (decentralized wallet).

j. 1/26/2023: 104,361 USDT sent from 0x070a83 to 0x80A6A5 (decentralized wallet).

k. 1/29/2023: 102,881 USDT sent from 0x80A6A5 to 0x9ac05F (decentralized wallet). While in this wallet the USDT is comingled with additional funds.

l. 1/30/2023: 146,814 USDT sent from 0x9ac05F to 0x6cF5f4 (decentralized wallet). While in this wallet the USDT is comingled with additional funds.

m. 2/3/2023: 289,184 USDT sent from 0x6cF5f4 to 0x36a28b (decentralized wallet).

n. 2/25/2023: 242,360 USDT sent from 0x36a28b to 0x1fcd9d (decentralized wallet). While in this wallet the USDT is comingled with additional funds.

o. 2/25/2023: 400,000 USDT sent from 0x1fcd9d to 0x473f8D (decentralized wallet).

p. 3/4/2023 – 3/9/2023: 400,000 USDT sent, over four transactions, from 0x473f8D to 0x58D402 (decentralized wallet).

q. 3/6/2023: 99,286 USDT sent from 0x58D402 to 0xc746eF (decentralized wallet).

r. 3/9/2023: 43,834 USDT sent from 0xc746eF to 0x1d177F (decentralized wallet). While in this wallet the USDT is comingled with additional funds.

s. 3/22/2023: 2,000,000 USDT sent from 0x1d177F to 0x0bCd25 (decentralized wallet).

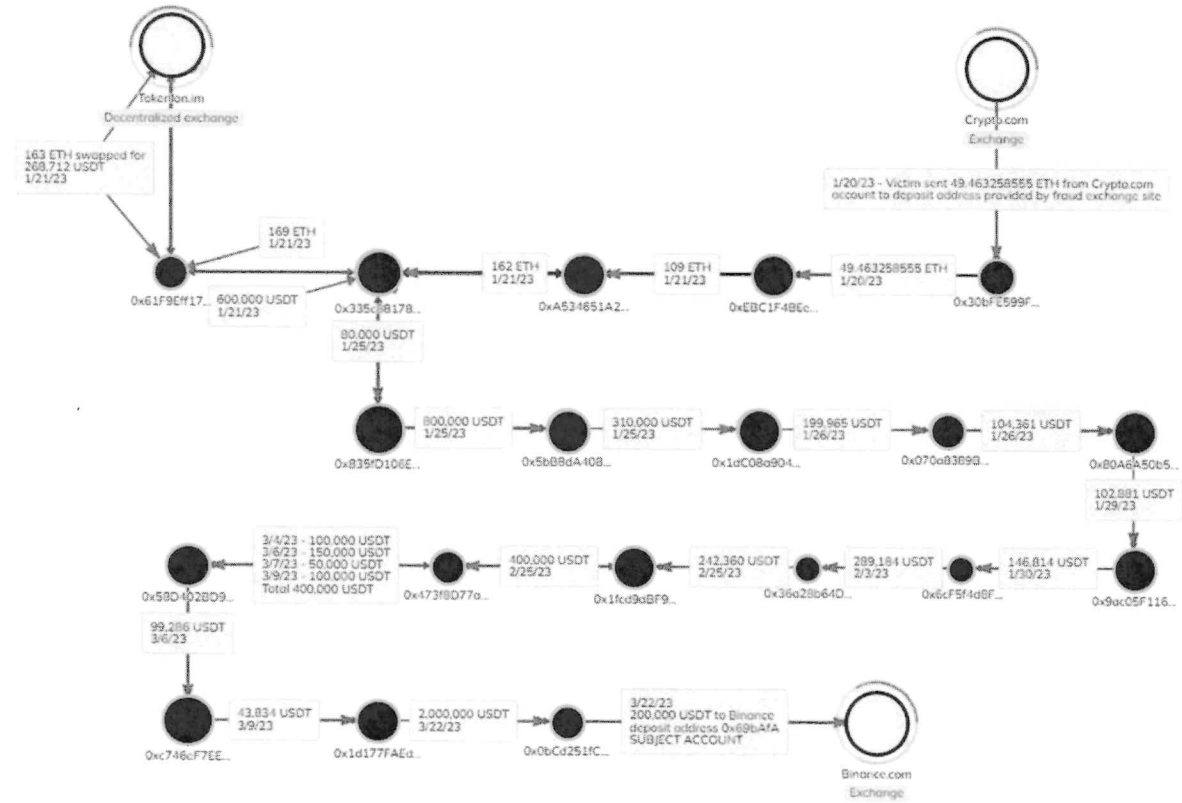
t. 3/22/2023: 200,000 USDT sent from 0x0bCd25 to 0x69bAfA (SUBJECT ACCOUNT at Binance).

23. The following is a graphical representation of the movement of funds from E.B.'s Crypto.com account to the SUBJECT ACCOUNT.

Yellow circles: Exchanges

Black circles: Decentralized wallets. The size of the circles indicates the relative number of transactions associated with that wallet (larger circle=more transactions).

Red arrows show the movement of the victim's funds.



24. On March 22, 2023, the USSS sent legal process to Binance requesting information on the account associated with deposit address 0x69bAfA. The account information received from Binance indicated that the owner of the account was Pan Xuexia. Binance provided a copy of Pan Xuexia's Resident Identity Card, issued by the People's Republic of China. Through e-mail correspondence with Pan Xuexia, she claimed that the 200,000 USDT deposit in her Binance account were the result of winnings on an online gambling site. She was not able to provide any documentation to substantiate this claim. Further analysis of the address from which the 200,000 USDT was received, 0x0bCd25, shows that it consistently received large round amounts of USDT from other decentralized wallets and subsequently sent out similar amounts to exchanges or other decentralized wallets. In my experience this pattern is indicative of money laundering activity and not of payouts of gambling sites, which tend to be smaller and of irregular amounts. Additionally, no blockchain analysis or tracing tool identified 0x0bCd25 as being associated with any known gambling site.

CONCLUSION

25. Based on the foregoing, probable cause exists to believe that the 39,991.998502 USDT virtual currency (formerly held in Binance Holdings Ltd. Account with User ID #28892515, belonging to Pan Xuexia, and associated with deposit address 0x69bAfA83E44057A5d6a2684aff4Bc361Fc09a5ef) constitutes or is derived from proceeds traceable to a wire fraud scheme executed in violation of 18 U.S.C. § 1343 and/or was involved in money laundering in violation of 18 U.S.C. § 1956 and/or 18 U.S.C. § 1957, and is therefore forfeitable to the United States pursuant to 18 U.S.C. § 981(a)(1)(C) and/or 18 U.S.C. 981(a)(1)(A).

26. The foregoing facts are furthermore sufficient to support a reasonable belief that the defendant property is forfeitable to the United States pursuant to 18 U.S.C. § 981(a)(1)(C) and/or 18 U.S.C. 981(a)(1)(A).

Executed this 3 day of June, 2024.

Timothy Williams
Senior Special Agent
United States Secret Service